FIX PROTOCOL LIMITED

Data Breach Policy

1. INTRODUCTION

1.1. Within the FIX Protocol Limited group of companies (together "FIX"), a large amount of Personal Data is stored, processed and shared. We are determined to ensure that Personal Data that we process is kept secure and confidential; this extends to third parties that act on our behalf.

1.2. This Policy applies to all Personal Data that we process and sets out the procedure that is to be followed in the event of a Personal Data Breach. This systematic approach must be used when responding to any reported Personal Data Breach in order to comply with reporting requirements under the Data Protection Law and also to mitigate the damage caused by the Personal Data Breach for the Data Subjects and us.

1.3. This Policy applies to all staff and we expect all staff to be familiar with the terms set out below.

1.4. Our Data Protection Manager is **Karen Biebuyck**, who is responsible for the day-to-day implementation of this Policy. However all staff are responsible for reporting actual or suspected Personal Data Breaches.

1.5. For the purpose of this Policy, Personal Data Breach is to cover both confirmed and suspected breaches.

2. DEFINITIONS

"**Data Breach Team**" shall consist of the following: Courtney McGuinn (Data Protection Manager) and all other members of the FIX Program Office team.

"**Data Protection Law**" shall mean (a) the Data Protection Act 1998; or (b) from 25th May 2018, the General Data Protection Regulation ((EU) 2016/679 ("GDPR"), read in conjunction with and subject to any applicable UK national legislation that provides for specifications or restrictions of the GDPR's rules; or (c) from the date of implementation, any applicable legislation that supersedes or replaces the GDPR in the UK or which applies the operation of the GDPR as if the GDPR were part of UK national law, which may include the Data Protection Act 2018.

"**Data Subjects**" shall have the meaning set out in the Data Protection Law.

"**DPM**" shall mean Data Protection Manager.

"**GDPR**" means the General Data Protection Regulation (Regulation (EU) 2016/679).

"**ICO**" shall mean the Information Commissioner's Office.

"**Personal Data**" shall have the meaning set out in the Data Protection Law.

"**Personal Data Breach**" shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. DETECTION OF PERSONAL DATA BREACHES

3.1. If any member of staff suspects a Personal Data Breach then they must inform the Data Breach Team immediately.

3.2. If required by the Data Breach Team, the reporting member of staff must complete the Incident Report Form (See Appendix 1).

3.3. Examples of a Personal Data Breach include:

3.3.1. loss or theft of data or equipment where Personal Data is stored;

3.3.2. unauthorised access to confidential data

3.3.3. disclosing Personal Data to an unauthorised recipient;

3.3.4. improper disposal of Personal Data;

3.3.5. hacking incidents; and

3.3.6. computer system error.

4. RESPONDING TO PERSONAL DATA BREACHES

4.1. Once the Data Breach Team has been alerted to a potential Personal Data Breach they must follow the below procedure:

Confirm the Personal Data Breach

- The Data Breach Team should identify whether data has been compromised and if the data constitutes Personal Data.
- Bearing in mind the sensitivity of the data, the potential severity of the breach and other relevant immediate factors, the Data Breach Team may proceed to containing the breach on the assumption that it is a Personal Data Breach before confirming.

Contain the Personal Data Breach

- The immediate priority is for Data Breach Team to identify the cause of the Personal Data Breach and establish whether there is the potential for a further Personal Data Breach.
- Steps must be taken to shut down the compromised system in order to prevent further loss and any further unauthorised access to the system.
- Where an unauthorised person has received Personal Data, that person should be contacted immediately and warned that the data they have received is Personal Data and they should not discuss it with anyone and must delete and destroy the Personal Data.

Attempt to recover the Personal Data

- The Data Breach Team must then establish whether anything can be done to recover any losses and limit the damage (e.g. physically recovering the data/equipment).

Conduct a Risk Assessment and Investigation

- An investigation of the Personal Data Breach will be undertaken by the Data Breach Team immediately and in any event within 24 hours of the Personal Data Breach being reported to the Data Breach Team.
- The Data Breach Team will investigate the Personal Data

Breach, assess the associated risks and prepare a report. The report will contain the following information:

- How the breach occurred;
- The type and volume of data involved;
- The identity of the Data Subjects affected;
- The number of Data Subjects affected;
- The sensitivity of the data breached;
- The protections that were in place;
- What the data could tell a third party and how it could be misused;
- Whether there is the potential harm that the Data Subjects could suffer; and
- Whether there are wider consequences of the breach.

5. NOTIFICATION

5.1. The Data Breach Team will determine whether the breach is one which is required to be notified to the ICO, the Data Subjects and/or the Data Controller.

5.2. The Data Breach Team will have to assess this on a case-by-case basis. They must consider the following factors when determining whether any notification is required:

5.2.1. If there are any legal, contractual or regulatory requirements to notify;

5.2.2. Whether notification would help the Data Subject;

5.2.3. Whether notification would help prevent the unlawful or unauthorised use of the Personal Data;

5.2.4. If a large number of Data Subjects are affected or if the consequences are very serious then the Data Breach Team should consider notifying the ICO. The ICO should only notified in regards to Personal Data. For further guidance on when to notify the ICO the Data Breach must consult the ICO's public guidance. The Data Breach Team must notify the ICO within 72 hours of becoming aware of the breach.

5.2.5. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms then the Data Breach Team must notify those Data Subjects without undue delay.

5.2.6. The Data Breach Team must keep a record of all Personal Data Breaches and the steps that were taken following the Personal Data Breach.

6. INFORMATION TO INCLUDE IN AN ICO REPORT

6.1. If the Data Breach Team find that a report to the ICO is required then the following information will need to be included in the report:

6.1.1. A description of the nature of the Personal Data Breach including:

6.1.1.1. The categories and approximate number of individuals concerned; and

6.1.1.2. The categories and approximate number of Personal Data Records concerned;

6.1.2. The name and contact details of the Data Protection Officer;

6.1.3. A description of the likely consequences of the Personal Data Breach;

6.1.4. A description of the measured taken, proposed to be taken, to deal with the Personal Data Breach and the measures taken to mitigate the adverse effects.

7. INFORMATION TO INCLUDE IN A REPORT TO INDIVIDUALS

7.1. The name and contact details of the DPM;

7.2. A description of the likely consequences of the Personal Data Breach; and

7.3. A description of the measured taken, proposed to be taken, to deal with the Personal Data Breach and the measures taken to mitigate the adverse effects.

8. REVIEWING, EVALUATING AND UPDATING THIS POLICY

8.1. Following the Personal Data Breach, the Data Breach Team must:

8.1.1. establish whether there are any present or future risks by carrying out a full review of the data protection measures in place;

8.1.2. consider the weak points in the current measures in relation to the Personal Data that has been lost and the context of the Personal Data Breach;

8.1.3. consider weak points in the current training and awareness of staff and identify whether new policies are required to prevent future Personal Data Breaches; and

8.1.4. produce a report that summarises the findings and recommendations on the Personal Data Breach and how to prevent future Personal Data Breaches.

APPENDIX 1

DATA BREACH FORM

Section 1 – Notification of a data breach

- Before completing this Form you MUST inform the Data Protection Manager (Courtney McGuinn) or a member of the Data Breach Team of the suspected Personal Data Breach.
- This section is to be completed by the member of staff reporting the Personal Data Breach.

Notification of the data breach	
Name of person reporting the breach:	
Telephone number:	
Email address:	
Date you discovered the data breach:	
Date of the data breach (if known):	
Description of data breach	
Please provide a short description of the data breach, including: ▪ Number of people affected; ▪ The type of data lost; ▪ The risk of personal data being lost; and ▪ What, if any, action you have taken to limit the severity of the data breach.	

Section 2 – Confirmation of the receipt of a notification of data breach

- This section is to be completed by the Data Protection Manager or a member of the Data Breach Team.

Receipt of a notification of data breach	
Name of the person receiving the notification:	
I confirm that I am either the Data Protection Manager or a member of the Data Breach Team:	
I confirm that this data breach is being dealt with in accordance with the Data Breach Policy:	
Signed: Dated:	